Códigos Espaço-Temporais de Treliça Baseados na Teoria de Reticulados

Dijiani Ludovino Guanais, Edson Donizete de Carvalho e Jozué Vieira Filho

***Resumo*—Neste trabalho é proposto um procedimento para desenvolvimento de códigos espaço-temporal de treliça, com diversidade de modulação máxima, a partir de uma generalização da técnica de geração de quadrados latinos. Essa extensão é baseada em resultados da teoria de reticulados e de constelações de sinais casadas a grupos aditivos.**

Palavras-Chave*—*códigos espaço-temporal, constelações de sinais rotacionadas e diversidade de modulação.

***Abstract*—This work proposes a systematic procedure for developing space-time trellis codes with full diversity modulation which is based on the technique used for generating latin square. The proposed procedure is an extension of several results obtained from lattices theory and signals constellations matched to additive groups .**

***Keywords*—*space-time codes, rotation signals constellations, modulation diversity*.**

I. INTRODUÇÃO

O estudo de novos códigos é algo fundamental para o desenvolvimento de sistemas de comunicações sem fio cada vez mais eficientes, seja na capacidade de uso de canais, otimização no uso de espectro ou simplesmente robustez nas transmissões com baixa potência.

Considere um sistema de comunicação móvel com modelo de canal do tipo Rayleigh e desvanecimento plano quase-estático configurado com n_t antenas transmissoras e $n_r$antenas receptoras. Tarokh *et. al.* [1] demonstraram que a codificação espacial-temporal, obtida a partir dos estados de uma treliça, permite obter-se um sistema de comunicação eficiente, tanto em termos de potência como também em termos de largura de banda, considerando um canal ruidoso. Na literatura estes códigos são denominados de *códigos espaço-temporal de treliça (CETT)*, pois consideram simultaneamente diversidade espacial e temporal. Esta técnica tem despertado cada vez mais o interesse da comunidade da teoria de informação porque permite explorar de forma completa diversidade na transmissão e na recepção.

A codificação na dimensão do tempo garante que o ganho de diversidade seja atingido sem comprometer a taxa de transmissão. A cada instante de tempo t, n_t palavras-códigos complexas são transmitidas simultaneamente através de blocos de comprimento l, dados por $n_t(c_t^1, \dots, c_t^{n_t})$, para $t = 1, \dots, n_t$. O sinal recebido pela antena $j, j = 1,2, \dots, n_t$, corrompido pelo desvanecimento do canal é obtido pela seguinte equação:

$$r_t^j = \sum_{i=1}^{n} \propto_{i,j} c_j^i \sqrt{E_s} + \eta_t^j, \qquad (1)$$

onde E_s representa a energia média do sinal transmitido; η_t^j é o ruído aditivo Gaussiano branco complexo (do inglês: Additive White Gaussian Noise - AWGN) com média zero e variância *No/2* por dimensão; $\alpha_{i,j}$ denota o desvanecimento presente ao longo do caminho da i-ésima antena transmissora a j-ésima antena receptora.

Considerando que os CETT são definidos por estruturas de treliças, pode-se implementar uma decodificação usando o algoritmo de Viterbi, o qual faz uso da métrica Euclidiana. O ganho de codificação entre a i-ésima antena transmissora e a j-ésima antena receptora permanece constante durante um quadro de transmissão, mas muda de forma independente de um quadro para o outro.

Dado um par de palavras c e e, considere $P(c \to e)$ como sendo a probabilidade de um decodificador de máxima verossimilhança decidir erroneamente pela palavra código $e = e_1^1 e_1^2 \dots e_1^n e_2^1 e_2^2 \dots . e_2^n \dots e_l^1 e_l^2 \dots e_l^n$, dado que a palavra transmitida tenha sido $c = c_1^1 c_1^2 \dots c_1^n c_2^1 c_2^2 \dots . c_2^n \dots c_l^1 c_l^2 \dots c_l^n$. Assumindo que os parâmetros associados ao desvanecimento $\alpha_{i,j}$ sejam conhecidos, então pode-se mostrar que o limite superior da probabilidade $P\left(c \to e \middle| \alpha_{i,j}, i = 1,2, \dots, n, j = 1,2, \dots, m\right)$ é exponencial e igual a:

$$\frac{1}{2}\exp\left(-\frac{d^2(c,e)E_s}{4N_0}\right), \qquad (2)$$

Da equação (2) tem-se:

$$d^2(c,e) = \sum_{j=1}^{m}\sum_{t=1}^{l}\left|\sum_{j=1}^{n}\alpha_{i,j\left(c_t^i - e_t^i\right)}\right|^2 \qquad (3)$$

Desenvolvendo a Equação (2) obtém-se $d^2(c,e)$ na forma:

$$d^2(c,e) = \sum_{j=1}^{m}\sum_{i=1}^{n}\sum_{k=1}^{n}\alpha_{i,j}\,\overline{\alpha_{i,j}}\left(c_t^i - e_t^i\right)\overline{\left(c_t^i - e_t^i\right)}, \qquad (4)$$

onde a barra superior, como em $\bar{\boldsymbol{a}}$, representa complexo conjugado do elemento $\boldsymbol{a}$.

A equação (4) pode ser reescrita matricialmente como:

$$d^2(c,e) = \sum_{j=1}^{m}\Omega_j A\overline{\Omega_j}, \qquad (5)$$

onde $\Omega = \left(\alpha_{1,j}, \alpha_{2,j}, \dots, \alpha_{n,j}\right)$e $\bar{\Omega} = \left(\overline{\alpha_{1,j}}, \overline{\alpha_{2,j}} \dots, \overline{\alpha_{n,j}}\right)$. As entradas $A_{p,q}$ da matriz A são obtidas pelos produtos internos $A_{p,q} = \sum_{t=1}^{l}\left(c_t^p - e_t^p\right)\left(\overline{c_t^q - e_t^q}\right)$). Ao substituir $d^2(c,e)$ na Equação (5), verifica-se que a probabilidade de erro com relação ao par $P\left(c \to e \middle| \alpha_{i,j}, i = 1,2, \dots, n, j = 1,2, \dots, m\right)$ é limitada superiormente de acordo com a equação (2).

Departamento de Engenharia Elétrica, Feis-Unesp, CEP 15385-000, Ilha Solteira-SP, Brasil, email: dijiani@yahoo.com.br

Departamento de Matemática, Feis – Unesp, CEP 15385-000, Ilha Solteira-SP, Brasil, email: edson@mat.feis.unesp.br

Departamento de Engenharia Elétrica, Feis-Unesp, CEP 15385-000, Ilha Solteira-SP, Brasil, email: jozue@dee.feis.unesp.br

O ganho de diversidade é definido como o expoente da relação sinal/ruído (SNR) $\left(\frac{E_s}{4N_0}\right)$, e representa a inclinação da curva de probabilidade de erro versus a SNR.

Em [2], os autores obtiveram diversidade de modulação máxima para canais de comunicação do tipo Rayleigh com desvanecimento plano quase-estático via codificação espaço-temporal. Tal codificação foi realizada através de uma sequência de rótulos q_t^i dos estados de uma treliça dados por $q_t^1 q_t^2 \dots q_t^{nT}$, que são elementos de um grupo aditivo H de cardinalidade prima. Tais grupos foram denominados pelos autores de código de grupo. Já a decodificação foi feita através da métrica Euclidiana definida na Equação (3).

Neste trabalho mostra-se que o procedimento proposto em [2] é obtido como uma consequência natural dos rótulos dos estados da treliça serem provenientes de um código de grupo aditivo de cardinalidade prima, cujos elementos são identificados por sinais de uma constelação rotacionada provenientes dos reticulados $\mathbb{Z}^2$ e $\mathbb{A}_2$. Como consequência a diversidade de modulação máxima é atingida.

Através de resultados da teoria de reticulados e de constelações de sinais casadas a grupos aditivos provenientes dos reticulados $\mathbb{Z}^2$ e $\mathbb{A}_2$ [3] é proposta uma sistematização do procedimento de geração de códigos de grupos.

Por fim, mostra-se que o procedimento é verificado quando $p = 2$ ou $p \equiv 1 \bmod 4$ para as constelações de sinais que sejam provenientes do reticulado $\mathbb{Z}^2$, ou quando $p = 3$ ou $p \equiv 1 \bmod 6$, para as constelações de sinais que sejam provenientes do reticulado $\mathbb{A}_2$.

II. Reticulados e Constelação de Sinais

A. Reticulados

Um reticulado Λ é um conjunto infinito de pontos em $\mathbb{R}^n$ que herda uma estrutura de grupo aditivo, o que representa uma ferramenta algébrica-geométrico importante no estudo da teoria de informação, principalmente em problemas relacionados à teoria de códigos.

Diz-se que Λ é um reticulado de dimensão $\boldsymbol{n}$ completo em $\mathbb{R}^n$, se existe um conjunto de vetores dado por $\beta = \{v_1, \dots, v_n\}$ linearmente independente em $\mathbb{R}^n$, tal que, Λ seja gerado por β, isto é, $\Lambda = \{x = \sum_{i=1}^{m} \lambda_i v_i, \lambda_i \in \mathbb{Z}^n\}$. O conjunto β é chamado de base do reticulado. Neste trabalho, são considerados apenas os reticulados completos.

Associada a uma base β existe uma matriz geradora M de ordem $n \times n$, onde as n colunas são formadas pelos $\boldsymbol{n}$ vetores de base β e as $\boldsymbol{n}$ linhas são obtidas a partir das $\boldsymbol{n}$ coordenadas dos vetores da base β. Cada vetor $x = (x_1, \dots, x_n) \in \Lambda$ pode ser escrito na forma $x = \xi_1 v_1 + \cdots + \xi_n v_n = \xi M$, onde os elementos ξ_i são inteiros e $\xi = (\xi_1, \dots, \xi_n)$.

Define-se a norma N de um vetor $x \in \Lambda$ da seguinte forma:

$$N(x) = (\xi_1 v_1 + \cdots + \xi_n v_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} \xi_i \xi_j v_i v_j = \xi . G . \xi^{tr} = f(\xi), \quad (6)$$

onde $G = M . \overline{M}^{tr}$ e $\overline{M}^{tr}$ representa a matriz transposta conjugada de M.

A função $f(\xi)$ de $\mathbf{n}$ variáveis $\xi_1, \dots, \xi_n$ é chamada de forma quadrática associada ao reticulado Λ.

Exemplo II.1: O reticulado $\Lambda = \mathbb{Z}^2$ é gerado pela base $\beta = \{v_1, v_2\}$, onde $v_1 = (1,0)$ e $v_2 = (0,1)$ tem como matriz geradora

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

A forma quadrática associada a cada elemento $\xi \in \mathbb{Z}^2$ é dada por $f(\xi) = \xi_1^2 + \xi_2^2$. O reticulado $\mathbb{Z}^2$ é identificado de forma natural pelos inteiros de Gauss $\mathbb{Z}[i] = \{x + iy | x, y \in \mathbb{Z}\}$, onde $i^2 = -1$. Cada elemento $(x, y) \in \mathbb{Z}^2$ corresponde de forma biunívoca a um único elemento $x + iy \in \mathbb{Z}[i]$.

Exemplo II.2: O reticulado $\Lambda = \mathbb{A}_2$(também, conhecido por reticulado hexagonal) é gerado pela base $\beta = \{v_1, v_2\}$, onde $v_1 = (1,0)$ e $v_2 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ e tem como matriz geradora

$$M = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

A forma quadrática associada a cada elemento $\xi \in \mathbb{A}_2$ é dada por $f(\xi) = \xi_1^2 + \xi_1 \xi_2 + \xi_2^2$. O reticulado $\mathbb{A}_2$ é identificado de forma natural pelos inteiros de Eisenstein-Jacobi $\mathbb{Z}[\omega] = \{x + \omega y | x, y \in \mathbb{Z}\}$, onde $\omega = \frac{1+i\sqrt{3}}{2}$. Cada elemento $(x, y) \in \mathbb{A}_2$ corresponde de forma biunívoca a um único elemento $x + \omega y \in \mathbb{Z}[\omega]$.

B. Constelação de Sinais

Uma constelação de sinais U é um subconjunto discreto de pontos em $\mathbb{R}^n$.

A diversidade de um sistema de comunicações pode ser aumentada, usando-se constelações específicas de sinais, por meio de diversidade de modulação [3]. Tal diversidade pode ser definida como sendo o número mínimo de componentes distintas entre dois vetores de uma constelação de sinais S n-dimensional, ou seja, a distância mínima de Hamming em S. Geometricamente, a diversidade de modulação é caracterizada pela ação de uma rotação na constelação S, de modo que o número de componentes distintas seja máximo. A Fig. 1 ilustra bem este procedimento para uma constelação de sinais bidimensional com 4 sinais [3].

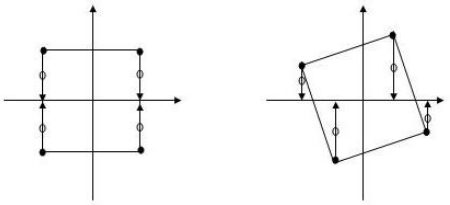

Fig. 1. Exemplo de constelação de sinais

As constelações de sinais obtidas via rotação são conhecidas por constelações de sinais rotacionadas. Em espaços euclidianos n-dimensionais, as constelações podem ser caracterizadas como um reticulado na forma cúbica do tipo $\mathbb{Z}^n$. Assim, um ponto x da constelação rotacionada é obtido pela ação de uma matriz M em u,ou seja, é o conjunto dos pontos $\{x = uM, u \in \mathbb{Z}^n\}$. No caso, bidimensional a matriz de rotação tem a forma

$M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, com $a, b \in \mathbb{Z}$, satisfazendo a condição $a^2 + b^2 = 1$.

Outra versão das constelações de sinais rotacionadas existentes em espaços euclidianos, mas apenas para os casos

que sejam da forma $2n$-dimensionais, são as constelações caracterizadas como um reticulado da forma $\mathbb{A}_2{}^n$. Assim, um ponto x da constelação rotacionada é obtido pela ação de uma matriz M em u, ou seja, é o conjunto dos pontos $\{x = uM, u \in \mathbb{A}_2{}^n\}$. No caso, bidimensional a matriz de rotação tem a forma:

$M = \begin{pmatrix} a & b \\ \frac{2a+b}{2} & -\frac{2b+a}{2} \end{pmatrix}$,com$a, b \in \mathbb{Z}$, satisfazendo a condição $a^2 + ab + b^2 = 1$.

Huber em [4], [5] e Nobrega *et.al.* em [6] propuseram procedimentos algébricos para se obter constelações de sinais casadas a grupos aditivos provenientes da estrutura aditiva dos corpos de Galois $GF(p)$. Esses procedimentos foram baseados em resultados clássicos da teoria dos números, na qual tem-se: se um inteiro primo p é escrito como soma de quadrados de inteiros, isto é, se $p = a^2 + b^2$, com $a, b \in \mathbb{Z}$, ou se p é escrito da forma $p = a^2 + ab + b^2$, com $a, b \in \mathbb{Z}$, então,

- dado um inteiro primo p, existe uma constelação de sinais U de cardinalidade p proveniente do reticulado $\mathbb{Z}[i]$ casada ao grupo aditivo G do corpo de Galois $GF(p)$ se $p = 2$ ou $p \equiv 1\ mod\ 4$ [4] e [6];
- dado um inteiro primo p, existe uma constelação de sinais U de cardinalidade p proveniente do reticulado $\mathbb{Z}[\omega]$ casada ao grupo aditivo de $GF(p)$ se $p = 3$ ou $p \equiv 1\ mod\ 6$ [5] e [6].

Carvalho *et. al.* [7] estendeu os resultados apresentados em [4],[5] e [6], mostrando que:

- dado um inteiro primo p, existe uma constelação de sinais U de cardinalidade p^n $(n \geq 1)$ casada a um grupo aditivo G de cardinalidade p^n, se $p = 2$ e $p \equiv 1\ mod\ 4$ ou se $p = 3$ e $p \equiv 1\ mod\ 6$ a partir dos reticulados $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente.

O procedimento proposto em [7] para se estabelecer um método de construção de uma constelação de sinais U de cardinalidade p^n, casada a um grupo aditivo G de cardinalidade p^n, equivale do ponto de vista algébrico, determinar ideais I em $\mathbb{Z}[\theta]$ (para $\theta = i$ ou ω) de norma relativa p^n, que satisfaçam à condição de que $G \simeq \mathbb{Z}[\theta]/I$.

Assim, os elementos de G podem ser vistos como classes de equivalências de $\mathbb{Z}[\theta]$, cujos representantes são dados por $0, \ldots, p^{n-1} - 1$. Desde que $\theta \in \mathbb{Z}[\theta]$, segue-se então que θ pertence a alguma classe lateral $\bar{s} \in \mathbb{Z}[\theta]/I$, com $0 \leq s \leq p^n - 1$, onde a norma relativa de θ é s. Ao tomar-se um dado elemento $x + y\theta$ pertence a alguma classe lateral $\bar{l} \in \mathbb{Z}[\theta]/I$, com norma relativa l, onde $0 \leq s \leq p^n - 1$, obtem-se, $\overline{x + y\theta} = \bar{x} + \overline{ys} = \overline{x + ys} = \bar{l}$.

Então, tem-se que:

$$x + y\theta \equiv l(mod I) \Leftrightarrow x + ys \equiv l(mod I) \quad (7)$$

Assim, um elemento $l \in G$ é um rótulo de um ponto $x + y\theta \in \mathbb{Z}[\theta]$, se a equação $x + yr \equiv l(mod p^n)$ for satisfeita. Para tal, basta encontrar uma única solução $r \in \mathbb{Z}$ para a equação $x + ys \equiv 0(mod p^n)$, onde $0 \leq s \leq p^n - 1$ [4].

Exemplo II.1: Considere $p = 5$. Nota-se que existe um par de inteiros $(2,1)$ tal que $2^2 + 1^2 = 5$. Logo, existe um ideal $I = \langle 2 + i \rangle \in \mathbb{Z}[i]$ e uma constelação de S de cardinalidade 5 proveniente do reticulado $\mathbb{Z}[i]$, casada ao grupo aditivo do corpo de Galois $GF(5)$ isormofo ao grupo quociente $\mathbb{Z}[i]/I$.

Nota-se que $r = 3$ é uma solução inteira de $2 + s = 5$. Então, o rótulo do elemento $x + yi$ em $\mathbb{Z}[i]$ é obtido a partir da equação $x + 3y \equiv l mod 5$.

De forma análoga, considerando $p = 7$, encontra-se um par de inteiros $(2,1)$ tal que $2^2 + 2.1 + 1^2 = 7$. Para este caso, obtém-se uma constelação de sinais S de cardinalidade 7 a partir do reticulado $\mathbb{Z}[\omega]$, porém, casada ao grupo aditivo proveniente do corpo de Galois $GF(7)$ isomorfo ao grupo quociente $\mathbb{Z}[\omega]/I$, onde $I = \langle 2 + \omega \rangle$.

Motivados por aplicações em CETT, são consideradas constelações especiais de sinais de cardinalidade m^2 (com m sendo uma potência de um inteiro primo) a partir de reticulado $\mathbb{Z}[\theta]$(para $\theta = i$ ou ω). Porém, os pontos precisam ser rotulados por elementos de grupos quocientes aditivos G de cardinalidade p^n, como proposto em [7]. Em outros termos, assume-se $S = \{j + k\theta \in \mathbb{Z}[\theta], j \in \{0, \ldots, p^n - 1\};\ k \in \{0, \ldots, p^n - 1\}\}$.

A representação geométrica de S pode ser vista como um paralelogramo com p^n linhas e p^n colunas, onde os elementos da t-ésima linha são escritos na forma $j + t\theta$ com $j \in \{0, \ldots, p^n - 1\}$. Já os elementos da t-ésima coluna são escritos na forma $t + k\theta$ com $k \in \{0, \ldots, p^n - 1\}$.

Proposição II.1: Considere uma constelação de sinais S na qual os sinais sejam rotulados por elementos do grupo aditivo de G de cardinalidade p^n(com $n \geq 1$), onde p é um inteiro primo da forma $p = 2, 3$ ou $p \equiv 1 \pmod 4$ ou $p \equiv 1 \pmod 6$ provenientes dos reticulados $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$, respectivamente. Então:

1) O $mdc(p^n, r) = 1$, onde r é o inteiro obtido como solução da Equação (7), através do qual rotula-se um elemento $x + y\theta \in S$ no grupo G através da equação $x + yr \equiv l (\mathrm{mod} p^n)$.

2) Todos os p^n elementos distintos de uma linha qualquer de S recebem rótulos distintos no grupo G.
3) Todos os p^n elementos distintos de uma coluna qualquer de S recebem rótulos distintos no grupo G.

Demonstração:

1) Considere, inicialmente, $p = 2$ ou $p \equiv 1 \pmod 4$. De acordo com [4], existe um conjunto de sinais de cardinalidade p^n casado ao grupo aditivo G isomorfo de grupo quociente $\mathbb{Z}[i]/I$. O ideal I é gerado por $I = \langle u + iv \rangle = \langle (a + bi)^n \rangle$, onde o par de inteiros (a, b) é solução da forma quadrática $x^2 + y^2 = p$ e o par de inteiros (u, v) é solução da forma quadrática $x^2 + y^2 = p^n$. Um elemento $l \in G$ (de ordem p^n) é um rótulo de um elemento $x + yi \in \mathbb{Z}[i]$ se $x + yr \equiv l \bmod p^n$, onde $r \in \mathbb{Z}$, é a única solução (em s) da equação $x + ys \equiv 0 \bmod p^n$, onde $0 \leq s \leq p^n - 1$.

Supondo a relação r/p^n, deve existir algum $t \in \mathbb{Z}$ tal que $r = p^t$. Nota-se que se r satisfaz à desigualdade $0 < r < p^n$ e, também, é solução da equação: $u + p^t v \equiv 0 \bmod p^t$, então, conclui-se que $u + p^t v \equiv 0 \bmod p^t$, ou seja, $u \equiv 0 \bmod p^t$. Mas, $p^t v \equiv 0 mod p^t$. Dessa forma, obtém-se $u + p^t v \equiv 0 mod p^t$. Por outro lado, $p^n \equiv 0 mod p^t$.

Por meio da Equação (7), conclui-se que $r = p^r$ é de forma simultânea solução inteira das equações $u + vr = p^t$ e $u + vr = p^n$. Porém, isto ocorre se, e somente se, $p^t = p^n$, ou

melhor, se t = n. Voltando na equação $u + p^n v = p^n$, obtêm-se como par de soluções inteiras de forma quadrática $f(x,y) = x^2 + y^2 = p^n$. Isso leva a uma contradição do tipo $0^1 + 1^2 = p^n$. Conclui-se, assim, que **r** não divide p^n. Como $0 \leq r \leq p^n - 1$, segue-se então que $mdc(p^n, r) = 1$.

No caso de $p \equiv 1\,(mod 6)$, por meio de uma argumentação análoga ao caso de $p \equiv 1\,(\mathrm{mod}4)$, determina-se uma constelação de sinais S e mostra-se que $mdc(p^n, r) = 1$. Porém, neste caso o reticulado é $\mathbb{Z}[\omega]$.

2) Pela equação (7), o rótulo de um elemento $x + y\theta \in \mathbb{Z}[\theta]$ por um elemento $l \in G$é realizado através da equação $x + yr \equiv 0 mod p^n$, onde $0 < r \leq p^n - 1$. Nota-se que os p^nelementos de uma linha qualquer de S são escritos na forma $j + t\theta$, para um certo índice j fixo, que pode assumir valores entre $j \in \{0, \dots, p^n - 1\}$. Suponha que dois elementos quaisquer de uma linha de $S, e + t\theta$ e $d + t\theta$, recebem o mesmo rótulo l em G, onde $e, d \in \{0, \dots, p^n - 1\}$. Então $e + tr \equiv d + tr \equiv l mod p^n$. Isso implica $p^n/(e - d)$. Desde que $0 \leq e, d \leq p^n - 1$, segue-se então que $d = e$. Logo, conclui-se que dois elementos quaisquer distintos de uma linha de S recebem rótulos distintos em G, o que prova o item (2).
3) Esta prova é bem similar à feita no item (2). Suponha que dois elementos quaisquer de uma coluna de $S, t + e\theta$ e $t + d\theta$ recebam o mesmo rótulo l em G, onde $e, d \in \{0, \dots, p^n - 1\}$. Então, tem-se $t + er \equiv t + dr \equiv l mod p^n$. Segue-se, então que $p^n/r(e - d)$. Portanto, p^n/r ou $p^n/(e - d)$. Mas, sabe-se que o $mdc(p^n, r) = 1$, já que p é um inteiro primo e que $r \in \{0, \dots, p^n - 1\}$. Assim, conclui-se que $p^n/(e - d)$. Por outro lado, $0 \leq e, d \leq p^n - 1$, então $e = d$. Logo, a conclusão é que dois elementos quaisquer distintos de uma linha de S recebem rótulos distintos em G.

Exemplo II. 2: A Fig. 2 ilustra o rotulamento dos sinais de uma constelação $S \subset \mathbb{Z}[i]$ de cardinalidade 25 (como definida na *Proposição II.1)* por elementos do grupo aditivo G de cardinalidade 5 proveniente do corpo de Galois $GF(5)$.

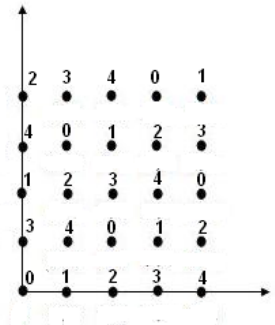

Fig. 2. Exemplo de constelação

Observação II.1

Deve-se observar que S pode ser visto como um conjunto formado por p^n vetores v_t, tal que, cada vetor v_t, seja formado pelas t-ésimas linhas da constelação de sinais e as coordenadas complexas j dada pelos pontos complexos $j + ti$, para $j \in \{0, \dots, p^n - 1\}$. Se a distância de Hamming for calculada a cada dois vetores de S, mostra-se facilmente que será igual a p^n.

III. Códigos espaço-Temporais Provenientes de Reticulados

Um quadrado latino pode ser caracterizado via um grupo aditivo H, onde em cada linha e coluna distinta em S há apenas um único elemento de H. Em [2], os autores mostraram que a existência dos quadrados latinos é uma consequência natural dos grupos aditivos módulo primo p serem cíclicos. Estes grupos foram denominados de códigos de grupo e, por meio desta técnica, a diversidade obtida é sempre máxima e igual a 2 no grupo H proveniente de uma constelação de sinais $em\ \mathbb{Z}[\theta]$.

Exemplo III.1: Para $p = 5$, e de acordo com o exemplo II.1, existe um par de inteiros $(2,1)$ tal que $2^2 + 1^2 = 5$. Tomando a operação aditiva módulo 5, mostra-se facilmente que o grupo aditivo $H = \{(0,0), (2,1), (4,2), (1,3), (3,4)\}$ é cíclico e gerado pelo elemento $(2,1)$, formando um quadrado latino, como ilustrado na Fig. 3.

	0	1	2	3	4
0	00				
1				13	
2		21			
3					34
4			42		

Fig. 3. Quadrado latino

Em cada transição foi realizada um rotulamento de sequências de n_T sinais da constelação S, denotada por $q_t^1 q_t^2 \dots q_t^{n_T}$ por meio dos elementos do código de grupo H.

Na decodificação foi utilizado o algoritmo de Viterbi para se calcular o caminho que gera a menor métrica acumulada. Neste sentido, tem-se:

$$\sum_{j=1}^{n_R} \left| y_t^j - \sum_{i=1}^{n_T} \propto_{ij} q_t^i \right|^2 \qquad (8)$$

Quando o sinal y_t^j é recebido na j-ésima antena de instante de tempo t, tem-se a sequência de rótulos $q_t^1 q_t^2 \dots q_t^{n_T}$, assumindo que a informação a respeito do canal é conhecida, ou seja, que os ganhos de percursos são conhecidos pelo decodificador.

Em geral, como os rótulos das transições desses códigos de treliças apresentam duas componentes, o sistema de comunicação possui duas antenas de transmissão, sendo que cada uma delas é usada para transmitir uma componente.

Apresenta-se a seguir o algoritmo proposto em [2] para estabelecer o maior d_{free}(distância livre na treliça obtida pela sequência de rótulos) e, consequentemente, obter a maior diversidade de modulação para os CETT a partir das constelações de sinais do tipo na treliça S.

Algorítmo de Construção [2]

Passo1) Deve-se aplicar a técnica de recobrimento espacial baseado em reticulados e, assim, obter código de grupo com a maior diversidade possível, isto é, será obtido um quadrado latino. Caso contrário ir para o passo 3.

Passo 2) A segunda componente da palavra-código será usada como referência no rotulamento dos ramos da treliça com os elementos do código de grupo H do código espaço-temporal associado. Nesta situação, quando submetido a canais com desvanecimento do tipo Rayleigh a $d_{free} > 2$, o código apresentará um melhor desempenho comparado com o caso trivial em que um quadrado latino não é obtido.

Passo 3) As transições da treliça que partem do i-ésimo estado terão a primeira componente igual a i e a segunda componente será rotulada sucessivamente com os elementos de H. Neste caso, quando submetidos a canais com desvanecimento do tipo Rayleigh a $d_{free} = 2$, não se obtém quadrado latino e a solução será sempre trivial.

Pelo procedimento de codificação proposto em [2], a partir dos grupos cíclicos de cardinalidade **m**, obtem-se **m** palavras. Se duas palavras forem comparadas, os rótulos das transições desses códigos de treliças numa mesma posição diferem em apenas uma posição e nunca em duas. Nesta situação, os autores obtinham diversidade máxima para os CETT.

Exemplo III.1: Para o caso p=5, após a aplicação da técnica dos quadrados latinos, obtém-se o diagrama apresentado na Fig. 4.

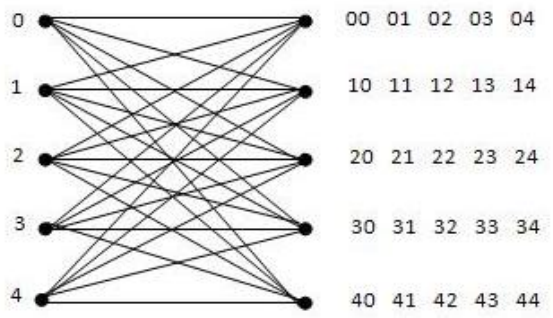

Fig. 4 Ilustração do exemplo III.1

Denotemos por K o quadrado latino. Note K pode ser visto como um subconjunto de uma constelação S como definida na Proposição II.1, onde cada elemento do quadrado latino da forma (a, b) é identificado pelo elemento da forma $a + b\theta$ do reticulado $\mathbb{Z}[\theta]$.

Como consequência desta identificação, estabelece-se o seguinte resultado.

Proposição III.1: Seja S uma constelação de sinais S como definida na Proposição II.1 casada a um grupo aditivo G de cardinalidade m , onde m é a potência de inteiro primo. Então, o conjunto dos sinais K de S que recebem como rótulos o elemento 0 do grupo aditivo G formam um grupo aditivo cíclico sob a operação módulo m .

Demonstração: Seja $a + b\theta \in \mathbb{Z}[\theta]$ obtida das soluções inteiras da forma quadrática $f(x_{1,} x_2) = x_1^2 + x_2^2$=m, se $\theta = i$, ou da forma quadrática $f(x_{1,} x_2) = x_1^2 + x_1x_2 + x_2^2$ =m, se $\theta = \omega$.

Mostra-se que tomando a soma modulo **m** obtém-se um grupo aditivo cíclico H $=< a + b\,\theta >$ de cardinalidade m.

Identificando o elemento $a + b\,\theta$ por (a, b) e realizando a adição (a, b) mod m, ao se considerar a soma de forma separada para cada coordenada mod m, obtém-se m elementos distintos. como consequência do fato do $mdc(a, m) = 1$ e de que o $mdc(b, m) = 1$. Assim, obtém-se m elementos distintos em cada coordenada que formarão um grupo cíclico H. Observe que cada elementoc $+$ d $\theta \in H$ é obtido da forma c + d $\theta = q$(a + b θ) para algum q $\in \{1, \dots, m-1\}$. Logo, se for considerada a função de rotulamento definida pela Equação (5), obtém-se $c + dr \equiv q(a + br)(mod m) \equiv q0(mod m), \equiv 0(mod m)$

Corolário III.1: A constelação de sinais K de cardinalidade $m = p^n$ como definida na Proposição III.1 para os casos em que $p = 2$, ou p $\equiv 1 \pmod 4$ a partir do reticulado $\mathbb{Z}[i]$, ou se $p = 3$ ou p $\equiv 1 \pmod 6$ a partir do reticulado $\mathbb{Z}[\omega]$, obtém-se uma constelação de sinais rotacionada e, consequentemente, os códigos CEET gerados apresentam diversidade de modulação máxima.

Demonstração: É uma consequência imediata das Proposições II.1 e III.1 e da Observação II.1.

IV Conclusões

Como consequência dos resultados obtidos em [7] via a técnica de casamento de constelações de sinais por grupos aditivos provenientes dos reticulados $\mathbb{Z}^2$ e $\mathbb{A}_2$, propôs-se um procedimento de construção de CETT com diversidade de modulação máxima, como proposto em [2], cujos resultados podem ser usados como ferramenta útil nos estudos de novos códigos.

Referências

[1] V. Tarokh, N. Seshadri and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction,"*IEEE Trans. Inform. Theory*, vol.IT-44, No.2, pp.44-765, 1999.

[2] R. V. Dutra and R. Palazzo Jr., Construction of optimum space-time convolutional trellis codes based on cyclic codes over groups and fields, *IEEE International Symposium on Information Theory*, Vol. 1, pp.1-1, Switzerland, 2002.

[3] J.Boutros, E. Viterbo, "Signal space diversity: a power – and bandwidth - efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Inform.Theory*, vol.IT-44, pp. 1453-1467, July 1998.

[4] K. Huber, "Codes over Gaussian integers,"*IEEE Trans. Inform. Theory*, vol.IT-40, pp. 207-216, Jan.1994.

[5] K. Huber, "Codes over Eisenstein-Jacobi integers,"*Contemporary Mathematics*, vol.168, pp. 165-179, 1994.

[6] T.P. NóbregaNeto, J.C. Interlando, O.M. Favareto,M. Elia, and R. Palazzo Jr, "Lattice constellations and codes from quadratic number fields, "*IEEE Trans. Inform. Theory*, vol.IT-47, pp. 1514-1527, May 2001.

[7] E.D. Carvalho, R. Palazzo Jr. and M. Firer, On the Construction and Labelling of Geometrically Uniform Signal Sets in in $\mathbb{R}^2$ Matched to Additive Quotient Groups, *J. Appl.Math and Computing*,vol.27 (2008), 1-6.